Foreign Collection Methods: Indicators and Countermeasures

Most Commonly Used Collection Methods

If you suspect you, a coworker, or your company may have been targeted using this method, report it to your FSO immediately.

Common foreign collection methods include:

- Suspicious network activity and cyber threats
- Solicitation and direct request
- Attempted acquisition of technology
- Academic solicitation
- Foreign travel
- Foreign visits
- Insider threat

Suspicious Network Activity and Cyber Threats

Attempts to carry out intrusions into cleared contractor networks and exfiltrate protected information

Technique

An adversary may target anyone or any system at any facility, using a number of methods:

- Cyber intrusion
- Viruses
- Malware
- Backdoor attacks
- Acquisition of user names and passwords

Indicators

The following is a list of suspicious indicators related to suspicious network activity and cyber threats:

- Unauthorized system access attempts
- Unauthorized system access to or disclosure of information
- Any acts that interrupt or result in a denial of service
- Unauthorized data storage or transmission
- Unauthorized hardware and software modifications
- E-mails received from unknown senders (that include social engineering attempts such as phishing)

Countermeasures

The following countermeasures can be taken by cleared defense contractors to guard against this collection method:

- Comply with the measures in your company's Technology Control Plan (TCP)
- Conduct frequent computer audits
    - Ideally: Daily
    - At minimum: Weekly
- Do not rely on firewalls to protect against all attacks
- Report intrusion attempts
- Avoid responding to any unknown request and report these requests
- Disconnect computer system temporarily in the event of a severe attack

If you suspect you, a coworker, or your company may have been targeted using this method, contact your FSO. For additional information, refer to the Counterintelligence section of the DSS website at www.dss.mil.

Solicitation and Direct Request

Attempts by foreign entities to establish a connection with a cleared contractor vulnerable to the extraction of protected information

Technique

This method utilizes an information request from an unknown source that was not sought or encouraged. Examples include, but are not limited to: Sales, representation, agency offers, response to tenders for technical or business services, and requests under the guise of price quotes or marketing surveys.

Indicators

There are several possible indicators of unsolicited and direct requests, including, but not limited to, those listed below.

The requestor:

- Sends a request using a foreign address
- Has never met recipient
- Identifies self as a student or consultant
- Identifies employer as a foreign government
- States that work is being done for a foreign government or program
- Asks about a technology related to a defense program, project, or contract
- Asks questions about defense-related programs using acronyms specific to the program
- Insinuates the third party he/she works for is "classified" or otherwise sensitive
- Admits he/she could not get the information elsewhere because it was classified or controlled
- Advises the recipient to disregard the request if it causes a security problem, or the request is for information the recipient cannot provide due to security classification, export controls, etc.
- Advises the recipient not to worry about security concerns
- Assures the recipient that export licenses are not required or not a problem

Countermeasures

The following countermeasures can protect against this method:

- View unsolicited and direct requests with suspicion, especially those received via the Internet
- Respond only to people who are known after verifying their identity and address
- If the requester cannot be verified:
  - Do not respond in any way
  - Report the incident to security personnel

If you suspect you, a coworker, or your company may have been targeted using this method, contact your FSO. For additional information, refer to the Counterintelligence section of the DSS website at www.dss.mil.

Attempted Acquisition of Technology

Attempts to acquire protected information in the form of controlled technologies via direct purchase of firms, agency of front companies, and/or third countries

Technique

Examples include, but are not limited to, attempted purchases of: Equipment, plans, diagrams, spec sheets, and/or schematics.

Indicators

The following are suspicious indicators related to attempted acquisition of technology.

Initial request:

- The request is directed at an employee who does not know the sender and who is not in the sales or marketing office
- Solicitor is acting as a procurement agent for a foreign government
- Company requests technology outside the requestor's scope of business
- Individual has a lack of/no knowledge of the technical specifications of the requested type of technology

Order details:

- Vagueness of order: Quantity, delivery destination, or identity of customer
- Unusual quantity
- Requested modifications of technology
- Rushed delivery date

Shipping:

- End user is a warehouse or company that organizes shipments for others
- End user address is in a third country
- Address is an obscure PO Box or residence
- Multiple businesses are using the same address
- Buyer requests all products be shipped directly to him/her
- Requestor offers to pick up products rather than having them shipped

Countermeasures

The following countermeasures can be taken by cleared defense contractors to guard against this collection method:

- Comply with the measures in your company's Technology Control Plan (TCP)
- Avoid responding to any unknown request and report these requests
- Respond only to people who are known after verifying their identity and address
- If the requester cannot be verified:
    - Do not respond in any way
    - Report the incident to security personnel

If you suspect you, a coworker, or your company may have been targeted using this method, contact your FSO. For additional information, refer to the Counterintelligence section of the DSS website at www.dss.mil.

Academic Solicitation

Attempts to acquire protected information under the guise of academic reasons

Technique

Examples include, but are not limited to, requests for or arrangement of:

- Peer or scientific board reviews of academic papers or presentations
- Requests to study or consult with faculty members
- Applications for admission into academic institutions, departments, majors, or programs, as faculty members, students, fellows, or employees

Indicators

Collection efforts using academic solicitation may include, but are not limited to:

- U.S. academics receive:
  - Requests to provide dual-use components under the guise of academic research
  - Unsolicited emails from peers in their academic field soliciting assistance on fundamental and developing research
  - Invitations to attend or submit a paper for an international conference
  - Requests to review research papers, in hopes the expert will correct any mistakes
- Collection via foreign academics may involve:
  - Foreign students accepted to a U.S. university or at postgraduate research programs who are recruited by their home country to collect information, and may be offered state-sponsored scholarships as an incentive for their collection efforts
  - Overqualified candidates seeking to work in cleared laboratories as interns
  - Candidates seeking to work in cleared laboratories whose work is incompatible with the requesting individual's field of research

Countermeasures

The following countermeasures may guard against this collection method:

- Review all documents being transmitted; use a translator, when necessary
- Provide foreign representatives with stand-alone information systems
- Share the minimum amount of information appropriate to the scope of the research
- Be aware of project scope and how to handle and report elicitation
- Attend sustainment training
- Refuse to accept unnecessary foreign representatives into the facility
- Comply with the measures in your company's Technology Control Plan (TCP), including badging systems to identify both foreign and domestic visitors

If you suspect you, a coworker, or your company may have been targeted using this method, contact your FSO. For additional information, refer to the Counterintelligence section of the DSS website at www.dss.mil.

Foreign Travel

Attempts to acquire protected information via the exploitation of travelers

Technique

Examples include, but are not limited to:

- Transportation-related targeting
- Hotel surveillance
- Recruitment attempts

Indicators

Suspicious or inappropriate conduct related to foreign travel can include:

- Bugged hotel rooms or airline cabins
- Intercepts of communications and email transmissions
- Recording of telephone calls and/or conversations
- Unauthorized access and downloading, including outright theft of hardware and software
- Installation of malicious software
- Intrusions into or searches of hotel rooms, briefcases, luggage, etc.
- Recruitment attempts via bribery, blackmail, or coercion

Countermeasures

The following countermeasures can protect cleared defense contractors against this method:

- Do not publicize travel plans and limit sharing of this information to people who need to know
- Conduct pre-travel security briefings
- Maintain control of sensitive information, media, and equipment.
    - Do not pack these types of articles in checked baggage; carry them with you at all times.
    - Do not leave them unattended in hotel rooms or stored in hotel safes
- Keep hotel room doors locked; note how the room looks when you leave
- Limit sensitive discussions; public areas are rarely suitable for discussion of sensitive information
- Do not use information systems at foreign hotels or business centers for sensitive matters
- Ignore or deflect intrusive or suspect inquiries or conversations about professional or personal matters
- Keep unwanted sensitive material until it can be disposed of securely

If you suspect you, a coworker, or your company may have been targeted using this method, contact your FSO. For additional information, refer to the Counterintelligence section of the DSS website at www.dss.mil.

Foreign Visits

Attempts to gain access to and collect protected information that goes beyond that permitted and intended for sharing

Technique

Examples include, but are not limited to:

- Pre-arranged visits by foreign contingents
- Unannounced visits

Indicators

Suspicious or inappropriate conduct during foreign visits can include:

- Requests for information outside the scope approved for discussion
- Hidden agendas associated with the stated purpose of the visit
- Visitors/students requesting information and becoming irate upon denial
- Individuals bringing cameras and/or video equipment into areas where no photographs are allowed
- Individuals providing last minute changes to visitor list

Countermeasures

The following countermeasures can protect cleared defense contractors against unauthorized access by foreign visitors:

- Contractors may coordinate with DSS prior to visit
- Prior to visit: attend briefings on approved visit procedures
- Prior to visit: walk visitor route and identify vulnerabilities
- Be aware of restrictions on the visitors, and the nature of the threat
- Participate in post-visit debriefs
- Ensure visitors do not bring recording devices, including cell phones, into the facility

If you suspect you, a coworker, or your company may have been targeted using this method, contact your FSO. For additional information, refer to the Counterintelligence section of the DSS website at www.dss.mil.

Insider Threat

The insider threat has the potential to inflict the greatest damage of any collection method. Examples include espionage, terrorism, unauthorized disclosure of national security information, and loss or degradation of resources or capabilities.

Technique

Potential sources include:

- Employees
- Contractors
- Anyone with legitimate access to an organization

Indicators

The following are potential espionage indicators:

- Alcohol or other substance abuse or dependence
- Mental health issues
- Extreme, persistent interpersonal difficulties
- Hostile or vindictive behavior
- Criminal behavior
- Financial difficulties
- Unexplained or sudden affluence
- Unreported foreign contact and travel
- Inappropriate, unusual, or excessive interest in classified, sensitive, or proprietary information
- Misuse of information systems
- Divided loyalty or allegiance to the United States
- Work hours that are inconsistent with job assignment
- Repeated security violations
- Reluctance to take polygraph

Countermeasures

The following countermeasures can be taken by cleared defense contractors to guard against the insider threat:

- Request training on the insider threat
- Attend briefings on elicitation methods
- Be alert to actions of other employees
- Monitor the activities of foreign visitors for indications that they are targeting company personnel
- Report suspicious behaviors and activities including potential espionage indicators and signs of foreign targeting of personnel
- Limit the dissemination of sensitive information based on need-to-know
- Monitor classified systems for reportable anomalies

If you suspect you, a coworker, or your company may have been targeted using this method, contact your FSO. For additional information, refer to the Counterintelligence section of the DSS website at www.dss.mil.